(2) The following are some examples of personal information that should not be contained in group orders. The following list is not all-inclusive—

(i) Complete SSN;

(ii) Home addresses and phone numbers; or

(iii) Date of birth.

(i) *Disclosures for established routine uses.* (1) Records may be disclosed outside the DOD without the consent of the individual to whom they pertain for an established routine use.

(2) A routine use shall—

(i) Be compatible with and related to the purpose for which the record was compiled;

(ii) Identify the persons or organizations to which the records may be released; and

(iii) Have been published previously in the FEDERAL REGISTER.

(3) Establish a routine use for each user of the information outside the Department of Defense who needs official access to the records.

(4) Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the FEDERAL REGISTER at least 30 days before actually disclosing any records.

(5) In addition to the routine uses listed in the applicable systems of records notices, ''Blanket Routine Uses'' for all DOD maintained systems of records have been established. These ''Blanket Routine Uses'' are applicable to every record system maintained within the DOD unless specifically stated otherwise within a particular record system. The ''Blanket Routine Uses'' are listed at appendix C of this part.

(j) *Disclosure accounting.* (1) System managers must keep an accurate record of all disclosures made from DA Privacy Act system of records, including those made with the consent of the individual, except when records are—

(i) Disclosed to DOD officials who have a ''need to know'' the information to perform official government duties; or

(ii) Required to be disclosed under the Freedom of Information Act.

(2) The purpose for the accounting of disclosure is to—

(i) Enable an individual to ascertain those persons or agencies that have received information about them;

(ii) Enable the DA to notify past recipients of subsequent amendments or ''Statements of Dispute'' concerning the record; and

(iii) Provide a record of DA compliance with the Privacy Act of 1974, if necessary.

(3) Since the characteristics of records maintained within DA vary widely, no uniform method for keeping the disclosure accounting is prescribed.

(4) Essential elements to include in each disclosure accounting report are—

(i) The name, position title, and address of the person making the disclosure;

(ii) Description of the record disclosed;

(iii) The date, method, and purpose of the disclosure; and

(iv) The name, position title, and address of the person or agency to which the disclosure was made.

(5) The record subject has the right of access to the disclosure accounting except when—

(i) The disclosure was made for law enforcement purposes under 5 U.S.C. 552a(b)(7); or

(ii) The disclosure was made from a system of records for which an exemption from 5 U.S.C. 552a(c)(3) has been claimed.

(6) There are no approved filing procedures for the disclosure of accounting records; however, system managers must be able to retrieve upon request. With this said, keep disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

(7) When an individual requests such an accounting, the system manager or designee will respond within 20 working days.

§ 505.8 Training requirements.

(a) *Training.* (1) The Privacy Act requires all heads of Army Staff agencies, field operating agencies, direct reporting units, Major Commands, subordinate commands, and installations to establish rules of conduct for all personnel involved in the design, development, operation, and maintenance of any Privacy Act system of records and

to train the appropriate personnel with respect to the privacy rules including the penalties for non-compliance (See 5 U.S.C. 552a(e)(9)).

(2) To meet the training requirements, three general levels of training must be established. They are—

(i) *Orientation.* Training that provides basic understanding of this part as it applies to the individual's job performance. This training will be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training;

(ii) *Specialized training.* Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to, personnel specialists, finance officers, DOD personnel who may be expected to deal with the news media or the public, special investigators, paperwork managers, individuals working with medical and security records, records managers, computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, contractors and anyone responsible for implementing or carrying out functions under this part. Specialized training should be provided on a periodic basis; and

(iii) *Managerial training.* Training designed to identify for responsible managers (such as senior system managers, Denial Authorities, and functional managers described in this section) issues that they should consider when making management decisions affected by the Privacy Act Program.

(b) *Training tools.* Helpful resources include—

(1) Privacy Act training slides for Major Commands and Privacy Act Officers: Contact the DA FOIA/P Office, or slides can be accessed at the Web site *https://www.rmda.belvoir.army.mil/rmdaxml/rmda/FPHomePage.asp.*

(2) The ''DOJ Freedom of Information Act Guide and Privacy Act Overview'': The U.S. Department of Justice, Executive Office for United States Attorneys, Office of Legal Education, 600 E. Street, NW., Room 7600, Washington, DC 20530, or training programs can be accessed at the Web site *www.usdoj.gov/usao/eousa/ole.html.*

§ 505.9 Reporting requirements.

The Department of the Army will submit reports, consistent with the requirements of DOD 5400.11–R, OMB Circular A–130, and as otherwise directed by the Defense Privacy Office. Contact the DA FOIA/P Office for further guidance regarding reporting requirements.

§ 505.10 Use and establishment of exemptions.

(a) *Three types of exemptions.* (1) There are three types of exemptions applicable to an individual's right to access permitted by the Privacy Act. They are the Special, General, and Specific exemptions.

(2) Special exemption (d)(5)—Relieves systems of records from the access provision of the Privacy Act only. This exemption applies to information compiled in reasonable anticipation of a civil action or proceeding.

(3) General exemption (j)(2)—Relieves systems of records from most requirements of the Act. Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim this exemption.

(4) Specific exemptions (k)(1)–(k)(7)–Relieves systems of records from only a few provisions of the Act.

(5) To find out if an exemption is available for a particular record, refer to the applicable system of records notices. System of records notices will state which exemptions apply to a particular type of record. System of records notices that are applicable to the Army are contained in DA Pam 25–51 (available at the Army Publishing Directorate Web site *http://www.usapa.army.mil/*), the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy/*), or in this section). Some of the system of records notices apply only to the Army and the DOD and some notices are applicable government-wide.

(6) Descriptions of current exemptions are listed in detail at appendix C of this part.

(b) *Exemption procedures.* (1) For the General and Specific exemptions to be applicable to the Army, the Secretary